

### Remarks

Reconsideration and allowance of this application are respectfully requested in view of the above amendments and the following remarks.

The claims were rejected under 35 U.S.C. 103(a) as unpatentable over Talati, et al., United States Patent No. 5,903,878, in view of Teper, et al. United States Patent No. 5,815,665, with various secondary references being added with respect to some of the dependent claims. The rejections are traversed. Applicants' invention, as set forth in the claims, is neither shown nor suggested by the references, whether the references be considered one at a time or in combination.

The claimed invention relates to a method of ordering, paying for, and delivering goods on a mobile network, such as a cellular telephone network. The Office contends that Teper discloses transactions conducted through a Web site on the Internet and contends that the Web site is a network operator providing the services required to initiate and conduct a transaction. *Assuming Teper to disclose that*, still, the combination of Talati and Teper *does not* suggest or otherwise make obvious the claimed invention since Teper makes no showing or suggestion of a mobile network. Teper shows or suggests only a Web based method. The claims have been amended to make clear that the claimed invention relates to a mobile network, which for example might be a cellular telephone network, thus patentably distinguishing from the combination of Talati and Teper and the other references.

With regard to claims 3, 39, and 51, the Office action contends that Teper discloses the exchange of encrypted messages throughout sessions for the purpose of authentication, and contends that it is known that for each transaction

unique service request numbers must be generated to track the individual transactions. However, in the claimed invention calculating a second service response value relates to a detailed authentication process. The second service response value has nothing to do with unique service request numbers. Teper might be regarded as disclosing the idea of a unique but anonymous sessions ID, but Teper does not teach how that it created.

With regard to claim 13, the Office Action contends that in column 3 Talati teaches about unique transaction identifiers and suitable encryption methods or a set of virtual keys, which incorporate random numbers. Nevertheless, Talati does not show or suggest determining whether service response values match, and transmitting the content to the user when the service response values do match, as in claim 13.

With regard to claim 25, the Office Action contends that in column 3 Talati teaches about the use of suitable encryption methods and contends that communication between the different parties may be encrypted. In lines 56-58 of column 3, Talati states that the delivery and communication systems between the client, merchant, and the transaction administrator preferably consist of some type of computer network such as the Internet, a private Intranet, or any suitable network. Talati only suggests encrypting the validation request sent from the transaction administrator to the client and the confirmation of the validation sent from the client to the transaction administration. Talati does not show or suggest the particulars of claim 25.

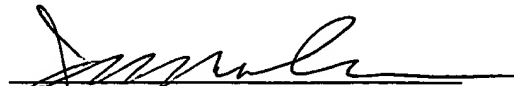
It is accordingly submitted that the claims distinguish patentably from the references and are allowable.

In view of the above amendment and the remarks, it is respectfully urged that all of the grounds for objection and rejection have been overcome, that the claims distinguish patentably from the references and are allowable, and that the application is in condition for allowance.

Attached hereto is a marked-up version of the changes made to the claim 13 by the current amendment. The attached pages are captioned **"Version with markings to show changes made."**

To the extent necessary, Applicants petition for an extension of time under 37 CFR §1.136. Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 01-2135 (Case No. 0171.37999X00) and please credit any excess fees to such deposit account.

Respectfully submitted,



James N. Dresser  
Registration No. 22,973  
ANTONELLI, TERRY, STOUT & KRAUS, LLP

JND

14/B

VERSION WITH MARKINGS TO SHOW CHANGES MADE

1. (Amended) A method of ordering, paying for and delivering goods and services, comprising:

ordering and paying for a content by a user selected from a content provider;

transmitting a first service response value calculated by the user to the content provider;

calculating a second service response value by ~~a network operator~~ mobile network operator when the user requests the content from the ~~network operator~~ mobile network operator;

verifying, by the ~~network operator~~ mobile network operator contacting the content provider, that the first service response value matches the second service response value; and

transmitting the content to the user by the ~~network operator~~ mobile network operator when the first service response value matches the second service response value.

3. (Amended) The method recited in claim 1, wherein the second service response value is calculated by the ~~network operator~~ mobile network operator based on the random number received from the user and a second secret key possessed by the ~~network operator~~ mobile network operator and associated with the user.

4. (Amended) The method recited in claim 2, wherein the first secret key is contained in a subscriber identification module provided by the ~~network operator~~ mobile network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key.

5. (Amended) The method recited in claim 3, wherein the second secret key is stored in an authentication center of a telecom infrastructure operated by the ~~network operator~~ mobile network operator and the first secret key and the second secret key are identical and assigned when the user subscribes for a telecommunication service provided by the ~~network operator~~ mobile network operator.

9. (Amended) The method recited in claim 7, wherein the content is encrypted by the ~~network operator~~ mobile network operator using a cipher key, calculated by an A8 algorithm module based on the random number and the second secret key, prior to transmitting the content to the user.

13. (Twice amended) A method of ordering, paying for and delivering goods and services, comprising:

ordering a content having a content ID by a user selected from a content provider;

transmitting a first service response value, a mobile network identifier, and a cipher key by the user to the content provider;

transmitting the first service response value, the mobile network identifier, and a random number to ~~a network operator~~ mobile network operator by the content provider;

calculating a second service response value and a cipher key by ~~a network operator~~ mobile network operator and determining if the first service response value matches the second service response value; and

transmitting the content to the user, when the first service response value matches second service response value, by the content provider.

14. (Amended) The method recited in claim 13, wherein the first service response value is calculated by the user based on a random number supplied by the content provider and a first secret key contained in a subscriber identification module provided by the ~~network operator~~ mobile network operator and contained in a mobile station.

16. (Amended) The method recited in claim 14, wherein the first secret key is not accessible directly by the user or the mobile station and the value of the secret key may not be discovered by the user, but is identical to the second secret key and both the first secret key and the second secret key are assigned when the user subscribes for a telecommunication service provided by the ~~network operator~~ mobile network operator.

20. (Amended) The method recited in claim 18, wherein the content is encrypted by the ~~network operator~~ mobile network operator using the cipher key,

calculated by an A8 algorithm module based on the random number and the second secret key, prior to transmitting the content to the user.

22. (Amended) The method recited in claim 13, wherein the user is billed by the ~~network operator~~ mobile network operator for the content in a telephone bill.

23. (Amended) The method recited in claim 13, further comprising:  
hashing, by the user, a price of the content, the random number and a seller ID to create a hashed number;

computing, by the user, the first service response value based on the secret key and the hashed random number;

transmitting, by the user, the first service response value to the content provider;

transmitting, by the content provider, the random number, the seller ID the price of the content and the first service response to the ~~network operator~~ mobile network operator;

computing, by the ~~network operator~~ mobile network operator, the second service response value based on the secret key, the price transmitted by the content provider and the random number;

verifying, by the ~~network operator~~ mobile network operator that the first service response value matches the second service response value; and

billing the user, by the ~~network operator~~ mobile network operator, the price when the first service response value matches the second service response value in a telephone bill.

25. (Amended) A method of ordering, paying for and delivering goods and services, comprising:

ordering a content from a ~~network operator~~ mobile network operator,  
having a content ID selected by a user;

transmitting a first service response value calculated by the user to the  
~~network operator~~ mobile network operator;

calculating a second service response value and a cipher key by a ~~network operator~~ mobile network operator and determining if the first service response value matches the second service response value;

transmitting the content ID, and a cipher key to the content provider; and

transmitting the content to the user by the content provider when requested by the user.

26. (Amended) The method recited in claim 25, wherein the first service response value is calculated by the user based on a random number supplied by the ~~network operator~~ mobile network operator and a first secret key possessed by the user.

27. (Amended) The method recited in claim 25, wherein the second service response value is calculated by the ~~network operator~~ mobile network operator based on the random number and a second secret key possessed by the ~~network operator~~ mobile network operator and associated with the user.



28. (Amended) The method recited in claim 26, wherein the first secret key is contained in a subscriber identification module provided by the ~~network operator~~ mobile network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key.

29. (Amended) The method recited in claim 27, wherein the second secret key is stored in an authentication center of a telecom infrastructure operated by the ~~network operator~~ mobile network operator and the first secret key and the second secret key are identical and assigned when the user subscribes for a telecommunication service provided by the ~~network operator~~ mobile network operator.

33. (Amended) The method recited in claim 31, wherein the content is encrypted by the content provider using a cipher key, calculated by an A8 algorithm module based on the random number and the second secret key and supplied by the ~~network operator~~ mobile network operator, prior to transmitting the content to the user.

36. (Amended) The method recited in claim 25, wherein the user is billed by the ~~network operator~~ mobile network operator for the content in a telephone bill.

37. (Amended) A method of ordering, paying for and delivering goods and services, comprising:

ordering a content, having a content ID, by a user selected from a ~~network operator~~ mobile network operator;

transmitting a first service response value calculated by the user to the ~~network operator~~ mobile network operator;

calculating a second service response value and a cipher key by a ~~network operator~~ mobile network operator and determining if the first service response value matches the second service response value; and

transmitting the content to the user by the ~~network operator~~ mobile network operator when requested by the user.

38. (Amended) The method recited in claim 37, wherein the first service response value is calculated by the user based on a random number supplied by the ~~network operator~~ mobile network operator and a first secret key possessed by the user.

39. (Amended) The method recited in claim 37, wherein the second service response value is calculated by the ~~network operator~~ mobile network operator based on the random number and a second secret key possessed by the ~~network operator~~ mobile network operator and associated with the user.

40. (Amended) The method recited in claim 38, wherein the first secret key is contained in a subscriber identification module provided by the ~~network operator~~ mobile network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key.

41. (Amended) The method recited in claim 39, wherein the second secret key is stored in an authentication center of a telecom infrastructure operated by the ~~network operator~~ mobile network operator and the first secret key and the second secret key are identical and assigned when the user subscribes for a telecommunication service provided by the ~~network operator~~ mobile network operator.

45. (Amended) The method recited in claim 43, wherein the content is encrypted by the ~~network operator~~ mobile network operator using a cipher key, calculated by an A8 algorithm module based on the random number and the second secret key and supplied by the ~~network operator~~ mobile network operator, prior to transmitting the content to the user.

46. (Amended) The method recited in claim 44, further comprising:  
decrypting the content received by from the ~~network operator~~ mobile network operator by the mobile station using an A8 algorithm module contained in the subscriber identification module of the mobile station to generate a cipher key based on the random number and the first secret key.

48. (Amended) The method recited in claim 37, wherein the user is billed by the ~~network operator~~ mobile network operator for the content in a telephone bill.

49. (Amended) A method of ordering, paying for and delivering goods and services, comprising:

ordering and paying for a plurality of contents by a user selected from a content provider;

transmitting a plurality of first service response values calculated by the user to the content provider;

calculating a plurality of second service response values by a ~~network operator~~ mobile network operator when the user requests the content from the ~~network operator~~ mobile network operator;

verifying, by the ~~network operator~~ mobile network operator contacting the content provider, that a one of the plurality of first service response values matches a one of the plurality of second service response values; and

transmitting a content of the plurality of contents to the user by the ~~network operator~~ mobile network operator when the one of the plurality of first service response values matches the one of the plurality of second service response values.

51. (Amended) The method recited in claim 49, wherein the plurality of second service response values are calculated by the ~~network operator~~ mobile network operator based on the plurality of random numbers received from the user and a second secret key possessed by the ~~network operator~~ mobile network operator and associated with the user.

52. (Amended) The method recited in claim 50, wherein the first secret key is contained in a subscriber identification module provided by the ~~network~~

~~operator~~ mobile network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key.

53. (Amended) The method recited in claim 51, wherein the second secret key is stored in an authentication center of a telecom infrastructure operated by the ~~network operator~~ mobile network operator and the first secret key and the second secret key are identical and assigned when the user subscribes for a telecommunication service provided by the ~~network operator~~ mobile network operator.

57. (Amended) The method recited in claim 55, wherein the content of the plurality of contents is encrypted by the ~~network operator~~ mobile network operator using a cipher key, calculated by an A8 algorithm module based on a random number of the plurality of random numbers and the second secret key, prior to transmitting the content of the plurality of contents to the user.